

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

FILED

DEC 02 2022

IN THE MATTER OF THE SEARCH
OF THE SNAPCHAT ACCOUNTS OF

anicholson_112

gmachine_e

adalyn_me

~~blrichert~~ DCP TE

existentialistj

LOCATED AT SNAPCHAT, INC.,

2772 DONALD DOUGLAS LOOP NORTH

SANTA MONICA, CA 90405

Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

Docket No. 3:22-mj-1234

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your affiant, Thomas Evans, an Investigator with the Knoxville Police Department (KPD) Internet Crimes Against Children (ICAC) Task Force and a Homeland Security Investigations (HSI) Task Force Officer, being duly sworn, deposes and states the following:

1. Your affiant has been employed with the KPD since January 22, 1996. Your affiant has been assigned to the Knoxville Police Department's Internet Crimes Against Children Task Force (KPD-ICAC) as a computer examiner and undercover online investigator for the past twenty-two years. As a KPD-ICAC Investigator and Homeland Security Task Force officer, your affiant is responsible for investigating and enforcing federal criminal statutes involving the sexual exploitation of children under Chapter 110 of Title 18, United States Code. Your affiant has acquired experience in these matters through specialized training and everyday work related to these types of investigations.

2. Your affiant has received the following training:

- 1996 Knoxville Police Department Training Academy Recruit Class A.
- 1997 Childhelp USA's Professional Training Conference.

- 1999 Protecting Children On-line provided by Fox Valley Technical College Criminal Justice Department, Appleton Wisconsin.
- 2000 Advanced Protecting Children On-line provided by Fox Valley Technical College, Criminal Justice Department.
- 2000 National Consortium of Justice Information and Statistics Training directed toward on-line investigation, tracking offenders and data recovery.
- 2000 40-hour course in the National White Collar Crime Data Recovery and Analysis.
- 2000 40-hour Internship with the Dallas Police Department's Internet Crimes Against Children Task Force.
- 40-hour internship with the Maryland State Police in October 2000 focusing on forensic software use in recovering computer-based evidence.
- 2001 Basic Class on EnCase computer forensic software.
- 2001 National Internet Crimes Against Children Training Conference in New Orleans focusing on the use of computer forensic utilities in evidence collection and Online Investigative Techniques.
- 2002 Crimes Against Children Conference in Dallas, TX focusing on online investigative techniques and computer forensic data recovery.
- 40-hour EnCase Intermediate Analysis and Reporting training in Sterling, VA April 2003.
- 2004 Silicon Valley ICAC Task Force Conference in San Jose, Ca with focus on online investigations and best computer forensic practices.

- 2004 Crimes Against Children Conference in Dallas, TX with emphasis on online investigative techniques and data recovery.
- December 2004 ICAC Investigative Techniques course in Knoxville, TN focusing on updated investigative techniques in online undercover operations.
- March 2005 EnCase Intermediate Analysis and Reporting course for computer examiners in Sterling, VA.
- May 2005 International Association of Computer Investigative Specialist 80-hour Forensic Computer Examiner Training Program in Orlando, FL.
- Recognized in April 2005 by the International Association of Computer Investigative Specialists as a Certified Electronic Evidence Collection Specialist.
- 2005 National ICAC Conference in Dallas, TX focusing on characteristics of the Internet offender and online undercover operations.
- Knoxville Police Department Basic Investigator Class January 30-February 3, 2006.
- 2006 National Crimes Against Children Conference in Dallas, TX focusing on online undercover Investigative Techniques.
- December 2006 FTK Boot camp held at Pellissippi State Technical College for computer forensic training using the Access Data Ultimate Toolkit software package.
- January 2007 Internet Crimes Against Children Task Force Operation Peer Precision Training in Tallahassee FL focusing on online undercover Peer-to-Peer investigations.
- June 12, 2008 F.B.I. CART ImageScan training concentrating on the use of the ImageScan System for secure computer previews and data recovery.

- April 11- May 14th 2010 United States Secret Service BCERT Computer Forensic training Hoover, AL.
- January 2011 assigned to the United States Secret Service Electronic Crimes Task Force for East Tennessee.
- February 21-23rd 2012 Tennessee ICAC Training conference in Nashville, TN focusing on cell phone investigations, human trafficking, undercover P2P investigations (instructed), and open source computer forensic tools.
- USDOJ 2012 National Law Enforcement Training Conference in Atlanta GA April 17-19th, 2012 focusing on P2P undercover investigations, Craigslist undercover investigations, Gigatribe investigations, and the psychological profile of a child pornography collector.
- June 13-17th Internship with the Citrus County Sheriff's Department regarding E Commerce undercover investigations (Operation Summer Nights).
- February 5th - 8th 2013 ICAC eMule P2P investigations.
- March 26-28th 2013– Tennessee ICAC state conference in Nashville, TN focusing on Commercial Sexual Exploitation of Children (CSEC).
- October 28-31, 2013 Tennessee ICAC state conference in Nashville, Tennessee, focusing on forensic preview tools, ICAC legal updates and virtual machine utilization for computer forensics and undercover investigations.
- February 24-26, 2014 – Tennessee ICAC state conference in Nashville, TN, focusing on computer previews, Google Security, and locating wireless devices.
- April 15-17, 2014 – 2014 Regional ICAC Law Enforcement Training on Child Exploitation focusing in court testimony, Ares Peer to Peer investigations, National Center for Missing and Exploited Children Law Enforcement Portal, and characteristics of the offender.

- September 18-19, 2014 – Westminster, Colorado ICAC BitTorrent Investigations.
- April 20-22, 2015 – Brentwood, Tennessee – Tennessee ICAC state conference focusing on online undercover chat investigations, legal updates, and human sex trafficking.
- November 11-13, 2015 – Gatlinburg, Tennessee – Tennessee ICAC conference focusing on current chat trends, P2P file sharing investigations, and on scene preview techniques and software.
- March 28-30, 2016 – Nashville, Tennessee – Tennessee ICAC conference focusing on legal updates, use of polygraph in conjunction with child pornography cases and online undercover operations.
- April 18, 2016 – Atlanta, Georgia – National ICAC Conference focusing on online undercover investigations, interviewing offenders, legal updates, psychology of the internet offender and on scene computer forensic tools.
- May 2, 2016 – Knoxville, Tennessee – Federal Bureau of Investigation Legal Training.
- October 17-19, 2016 – Chattanooga, Tennessee – Tennessee ICAC State Conference focusing on Legal Updates, Anonymity and Darknet, and IP Version 6.
- February 27- February 28, 2017 – Atlanta, Georgia – Darknet Training. Training focused on anonymous Darknet applications for the trafficking of child pornography.

3. I have received training and have experience related to Federal Criminal Procedures, federal statutes, and U.S. Customs Regulations. I have also received training and instruction in the investigation of child sexual exploitation, including child pornography

offenses. I have participated in numerous investigations related to the sexual exploitation of children. I have participated in numerous search warrants executed by HSI, as well as state and local police departments, and have participated in numerous seizures of computer systems and other evidence involving child exploitation and/or child pornography offenses. Your affiant has probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (production of child pornography), 18 U.S.C. §§ 2252(a) and 2252A(a) (transportation, receipt and/or distribution of child pornography) and 18 U.S.C. § 2252A(a) (possession of child pornography), are located on computers, computer servers, and/or electronic storage media located and under the control of Snap Inc. 2772 Donald Douglas Loop, North Santa Monica, CA 90405.

4. The information contained within this affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (production of child pornography), 18 U.S.C. §§ 2252(a) and 2252A(a) (transportation, receipt and/or distribution of child pornography) and 18 U.S.C. § 2252A(a) (possession of child pornography), are located on computers, digital devices, and/or electronic storage located and under the control of Snap Inc.

2772 Donald Douglas Loop, North Santa Monica, CA 90405 (as described with greater particularity in ATTACHMENT A).

GLOSSARY OF TERMS APPLICABLE TO THIS AFFIDAVIT

5. DARK WEB: A part of the Internet that is not indexed by traditional search engines such as Google. Dark Web sites cannot be located by traditional internet searches. Instead, Dark Web sites are intentionally hidden from public view and usually require certain software to access sites.

6. TOR BROWSER: The Tor browser is commonly used to access the Dark Web by routing a webpage request through multiple proxy servers. This rerouting through multiple proxy servers eliminates the ability to identify and trace the user's Internet Protocol Address (IP address).

7. THE INTERNET: The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across county, state, and national boundaries.

8. INTERNET PROTOCOL ADDRESS (commonly known as an "IP Address"): The unique numeric address of a machine or computer attached to and using the Internet. This address is displayed in four blocks of numbers (for example, 123.456.789.001). Each numeric address can be used by only one computer or device over the Internet at a time.

9. SNAPCHAT: Snapchat is a popular instant messaging application. A main feature of Snapchat is that pictures and messages are only available for a short period of time before they disappear and are no longer accessible to the recipient. Snapchat provides access to a worldwide computer network, commonly known as the Internet, to individuals and/or other users who have a subscription to, membership with, or affiliation with its company, organization, or commercial service. Snapchat also provides web hosting, email services, photo storage services, access solutions, etc. to its customers in which it reserves and/or maintains computer disk storage space on its own computer system servers for the use of the Internet Solutions subscribers/customers/users associated with its company. Items contained on this previously mentioned storage space can include electronic communications (commonly known as e-mail) between subscriber(s) and other parties, graphic image and/or text files, Internet history or Internet hyperlinks, file transfer protocol logs, website access logs, programs and other types of data or information stored in electronic form(s). Internet Service Companies, such as Snapchat, also maintain records pertaining to the individuals and/or other users who have subscriber accounts with their company. This information can include registration information, account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, news group access and posting information and other information both in computer data and written record format that records the activities of these accounts relating to the subscriber's use of the services offered by the Internet Service Company

**BACKGROUND INFORMATION CONCERNING
CHILD PORNOGRAPHY**

10. Based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers affect the methods used by people who possess, receive, distribute, and transport child pornography in these ways, among others:

a. Those that create child pornography can produce both still and moving images directly from a common video or digital camera, and other devices that create video and still images, including most cellular telephones and PDAs (e.g., a Blackberry). Images from such devices can be transferred to a computer by attaching the device to the computer using a cable, or by uploading images from the device's memory card directly onto the computer. Once on the computer, images can then be stored, manipulated, transferred, or printed. This includes transfer to some of the same types of devices that are commonly used to create child pornography, such as cellular telephones and PDAs, as well as computers. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography.

b. The Internet allows any computer to connect to another computer. Electronic contact can be made literally with millions of computers around the world. The Internet allows users, while still maintaining anonymity, to locate (i) other individuals with similar interests in child pornography and (ii) websites that offer images of child pornography.

Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. They can also distribute and collect child-pornography materials with peer-to-peer, or “P2P,” file sharing, which uses software to link computers together through the Internet to form a network that allows for the sharing of digital files among users on the network. These communication links allow contacts other individuals around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child-pornography collectors over the Internet.

c. The computer’s capability to store images in digital form makes it a common repository for child pornography. Internal and external computer hard drives typically store vast amounts of data, and hard drives with the capacity of 500 or more gigabytes – which can store tens of thousands of images at very high resolution – are not uncommon. Other electronic storage media, such as thumb drives and memory sticks, can store hundreds of images and dozens of videos. Likewise, optical storage media, which includes CD-ROMs and DVDs, and electromagnetic storage media, such as floppy disks, also can hold hundreds of images and multiple videos. Such electronic, optical, and electromagnetic storage media are very commonly used by those who collect child pornography to store images and videos depicting children engaged in sexually explicit activity. Agents who execute child pornography search warrants

often find electronic, optical, and/or electromagnetic storage media containing child pornography in the same location at or near the computer that was used to obtain, access, and/or store child pornography.

11. My training and experience, and the training and experience of other agents whom I have consulted, have shown me the following:

a. Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, computer graphics, or other types of images. Such individuals frequently store their child pornography on multiple electronic, optical, and/or electromagnetic storage media, including not only their computer, but also on external hard drives, disks, CD-ROMs, DVDs, memory sticks, thumb drives, cell phones, PDAs, and other such media. Many of these individuals also collect child erotica, which consist of items that may not rise to the level of child pornography, but which nonetheless serve a sexual purpose for those who have a sexual interest in children.

b. Individuals who produce, possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, Internet Relay Chat, newsgroups, instant messaging, and other similar interfaces. Additionally, individuals that use minors to

produce child pornography will often attempt to influence the minor into not disclosing the criminal activity. The perpetrator is often a trusted friend or family member making it very difficult for the victim to disclose to law enforcement.

c. Individuals who produce, possess, transport, receive, and/or distribute child pornography often collect, copy, or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in address books or notebooks, on computer storage devices, or merely on paper. In addition, individuals who produce child pornography may have various contact names and means of communication with the victim. Mobile applications, such as Snapchat, TikTok, Instagram and Facebook, are just a few of the applications used by suspects to communicate with like-minded individuals and victims.

d. The majority of individuals who possess, transport, receives, and/or distributes child pornography rarely, if ever, dispose of their sexually explicit materials and are known to retain their child pornography collections for long periods of time, even for years, in order to retain and gain access to child pornography that they have collected, sometimes with considerable effort. These individuals may go to great lengths to conceal and protect their collections of illicit materials from discovery, theft, and damage. These individuals almost

always maintain their collections in the privacy and security of their homes or other secure location. These individuals may keep their collections in locked containers including filing cabinets, safes, or lockboxes. These individuals may also maintain their collections in password-protected or encrypted electronic media. They may keep these passwords, and other information concerning their use of the computer, on handwritten or printed notes that they store in personal areas and around the computer.

e. Possessors, traders, and distributors of child pornography sometimes store their illegal images and videos online in remote storage accounts. Therefore, any records, documents, invoices and materials in any format or medium that relate to online storage or other remote computer storage could indicate that a person is storing illegal material in an online storage account.

THE INVESTIGATION

On January 5, 2021, your affiant received information from Homeland Security Chicago (HSI Chicago) regarding the possible production of child pornography and possible child sex abuse. HSI Chicago advised that a user associated with the screen names “Female4CP,” “2ndFemale4CP,” and “4thFemale4CP” was observed on the Dark Web site of “PublicPedoPub.” HSI Chicago advised that this user had uploaded an image of a nude minor female, who was photographed while shaving her legs in a bathtub. The image was assigned the

filename “IMGx6470x1x.jpg.” Corresponding communication at the time of the upload of the digital file, and identified with the screen names set forth above, indicated that the user was sexually abusing the minor female victim depicted in the uploaded photograph and that additional videos and images had recently been taken of the victim.

24. Through our investigation, Justis JOHNSON was identified as the suspect in the production of child pornography, distribution of child pornography, and the destruction or removal of property to prevent search and seizure. She subsequently was indicted on the same charges.

25. JOHNSON was able to destroy/alter items of evidence which included her Ace Laptop that she used for the distribution of child pornography as well as resetting her personal iPhone cell phone. During the examination of her one of her cell phones an image of your affiant’s police department business card was located. Your affiant had left a business card at JOHNSON’s place of employment (ServPro) with management as we attempted to identify where JOHNSON was working from during the COVID-19 pandemic. According to a witness that worked with JOHNSON, the card was located by JOHNSON in or around the desk of manager Chuck Peterson.

26. During our investigation, the Department of Children Services (DCS) permitted JOHNSON to visit with her 12-year-old daughter (hereinafter “AN”) – who was also a victim – but the visitation occurred only under strictly monitored conditions. Such visits occurred both in person and through video conferencing (i.e., Zoom). The purpose of the restricted contact was to

keep JOHNSON from manipulating and communicating with AN about the ongoing criminal case. Communication was restricted by order of the Juvenile Court to general topics and discussion of the ongoing criminal case was strictly prohibited. During this time, DCS documented numerous instances in which JOHNSON violated of the court-ordered restrictions in her communications with AN.

27. In December of 2021, AN was found to be in possession of a Samsung Galaxy A12 smartphone that she had purchased without the knowledge of her father, Robert Nicholson, who currently has custody of AN. The cell phone was brought to the Knoxville Police Department ICAC unit for examination, and Nicholson gave verbal and written consent to search the cell phone. Nicholson told investigators that AN had received \$300 - \$400 dollars from an unknown person. One day while she was being driven home from school, she told the driver that she needed to stop at Walmart to purchase some “feminine” products and that she preferred not to buy them with her father. While at Walmart, AN purchased the phone. Nicholson stated that he believed JOHNSON was responsible for getting the money to AN for purchase of the cell phone. He also stated he believed that AN had communicated with JOHNSON using the cell phone.

28. During the examination of the phone, the following Snapchat accounts were observed: “gmachine_e,” “Adalyn_me,” “blrichert,” and “existentialistj.” “Existentialistj” also had the designation of “Mom” in the contacts of AN’s phone. Based on the Snapchat communication on the phone of AN, “gmachine_e” appears to be Justis JOHNSON. Based on

the examination of the Samsung phone, it appears that both “gmachine_e” and “existentialist” are JOHNSON, “Adalyn_me” is AN, and “blrichert” is believed to be Biane McGee (JOHNSON’s aunt). McGee was assigned as the third-party custodian for JOHNSON after her detention hearing in the Middle District of Tennessee. JOHNSON violated the conditions of her release by utilizing cell phones and electronic devices while under the supervision of Biane McGee. Your affiant believes that it is possible that JOHNSON has communicated or attempted communication with AN through the Snapchat account of blrichert (Biane McGee). JOHNSON was found in violation of her pretrial release and, upon revocation of the release, she was placed in Laurel County Detention Facility Kentucky.

29. SnapChat communication found on the Samsung Galaxy A12 phone contains the following dialogue, which appears to be between AN (“Anicholson_112”) and JOHNSON (“Gmachine_e”):

Gmachine_e: Is this the best option? How many minutes or time do you have? Data? How can we get out

Anicholson_112: I have until the 14th of jan

Gmachine_e : If they found out about this I wouldn't be able to talk to you at all. So the signal app auto deletes like this app.

Gmachine_e: You aren't going to get caught?.... School knows you shouldn't have one either.

Anicholson_112: Yeah ik

Gmachine_e: Dude I think they're wanting Brandon to come to court in April as a witness?¹

Anicholson_112: Tf a witness to what omfg

Gmachine_e: A letter got sent from DCS. We need to do something because this has to end.

Anicholson_112: it better rnd..end

Gmachine_e: Blame it on them, "One time Priscilla was over and they all had my Snapchat logins, then they said they were going to ruing my life and make me a pornstar like my mom"...How's that?²

Anicholson_112: That's good

Gmachine_e: if we have someone to blame of anyone, this would end. Because they don't have anyone ... They did question all those girls and it's on their radar. And after I called DCS on porn on Priscilla's phone.

Anicholson_112: Lol

¹ "Brandon" apparently refers to Brandon Kavanaugh, JOHNSON's former boyfriend and her co-defendant.

² In this statement, it appears that JOHNSON is suggesting that AN fabricate a story to implicate her schoolmates.

Gmachine_e: I mean that. They know about it and me turning it into authorities and that Priscilla's mom was upset and Priscilla and them have called me so many times telling me to kill myself and they're going to ruin my life. Granddaddy went to your game that was canceled last night. He asked a principal about it being cancelled. The principal told Whitt. Whitt talked to Rachel today and lied and lied and lied about you not being able to see granddad.

Gmachine_e: Adalyn this is corrupt and will be a movie with a lawsuit suing DCS until then this a nightmare

Anicholson_112: I hate everyone who did this

Gmachine_e: So, get a damn story together like we had talked and call Sherry. I have her direct number too. And you tell her you think you know who did this and you want to talk to her in person and alone. I miss you so much. I'm sad every day. The babies are sad. This should be illegal.

Anicholson_112: I already told my therapist the story hoping she would say sum...But she didn't

Gmachine_e: Which story? And tell sherry you told your therapist too.

Anicholson_112: The one abt Brandon and that I think he did it

Gmachine_e: I say blame the girls. Kids, 12, 13 etc can't get in trouble. If you said you did this to sherry, or told her you uploaded something it would all be over... but then they would think you're lying "for me". I'd just add that you heard through kids from that school that Priscilla and whoever talked about getting into your Snapchat and sharing pictures. You have photos in your old private Snapchat. The girls got in there and have told people at the old school or you even in disappearing messages that they

shared your stuff.

Anicholson_112: I tried saying I did it and they told me that it wasn't a good choice to lie

Gmachine_e: Life or death here. Tell sherry you had these damn photos or video messages in your old Snapchat. And the girls got in. But you didn't want to get anyone in trouble or be in trouble so you thought this would go away. But now that you've heard from other people that the girls have told people you're upset and want this to end.

30. Based on your affiant's training and experience, the above Snapchat communication is between JOHNSON and AN. JOHNSON has been continually attempting to contact and manipulate the victim in this case to implicate someone other than JOHNSON in the production and possession of child pornography. In the above Snapchat communication JOHNSON ("gmachine_e") is advising the victim ("anicholson_112") to say that the child pornography images depicting AN, and uploaded to the Darkweb chat room of PublicPedoPub, were self-produced. In addition, JOHNSON is advising AN to spread the false story that girls at AN's school gained access to an old SnapChat account of AN and found the pornographic images, which they then uploaded to the Darkweb site. JOHNSON reassures AN that the girls will not get into any trouble because they are minors.

CONCLUSION

31. Based on the above information, your affiant respectfully submits that there is probable cause to believe that violations of 18 U.S.C. § 2251(a) (production of child pornography), 18 U.S.C. §§ 2252(a) and 2252A(a) (transportation, receipt and/or distribution of child pornography) and 18 U.S.C. § 2252A(a) (possession of child pornography) have been committed, and that evidence, instrumentalities, fruits, and contraband related to this criminal conduct, as further described in ATTACHMENT B, will be found in the location to be searched, as further described in ATTACHMENT A.

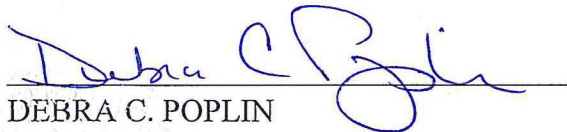
32. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See also* 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

33. Therefore, your affiant respectfully requests that this Court issue a search warrant for the property located at Snap Inc., 2772 Donald Douglas Loop, North Santa Monica, CA 90405, more particularly described in ATTACHMENT A, authorizing the seizure of the items described in ATTACHMENT B.

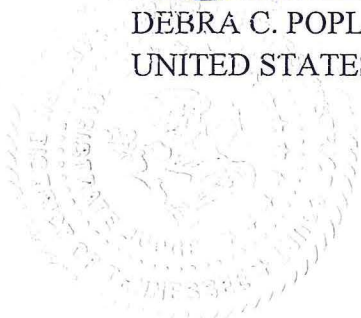


Thomas Evans
Investigator
Knoxville Police Department
Homeland Security TFO

Sworn and subscribed before me this 22nd day of November, 2022.



DEBRA C. POPLIN
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

Premises Location:

Snap Inc., 2772 Donald Douglas Loop, North Santa Monica, CA 90405

Snapchat accounts:

gmachine_e

Adalyn_me

~~Btriehert~~

anicholson_112

existentialistj

DCP TE

ATTACHMENT B

Below is a list of items to be searched and seized from the premises/accounts described in ATTACHMENT A:

a. All stored files, created, saved, or altered on or after January 1, 2021, maintained on the Snapchat server storage space, belonging to or associated with the above listed Snapchat user account(s). These files may include, but are not limited to: subscriber's full name(s), subscriber's address(es), subscriber's telephone number(s), e-mail address(es) associated with the subscriber(s), account or log-in name(s), any other information pertaining to the identity of the subscriber(s), billing information, credit card or payment information, types of services utilized by the subscriber and the lengths of such services or any other identifying or pertinent records relating to the subscriber, including IP addresses, dates and times of uploads of images if available.

b. All business records or files, created, saved, or altered on or after January 1, 2021, maintained on the Snapchat server storage space, belonging to or associated with the above listed Snapchat user account(s). These records may include, but are not limited to: account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, news group access and posting information and any other information, both in electronic computer data and written record format, that records the activities of these accounts relating to the subscriber's use of the services offered by the Internet Solutions Provider.

c. All stored electronic mail (e-mail) of any kind sent to, from, and/or through the e-mail address(es) of, belonging to, or associated with the above listed Snapchat user account(s), or through other associated accounts, on or after January 1, 2021. All stored electronic content created, saved, or altered on or after January 1, 2021, (including Internet history, file transfer

protocol logs, web access logs, electronically stored images, etc.) as well as all connection log files listing all account activity done by the subscriber/user associated with the above described Snapchat user account(s), including dates, times, methods of connecting (e.g. telnet, ftp, http, etc.), telephone dial-up connection records and any other connection information or Internet traffic data.

d. All chat logs of any kind, including but not limited to Snapchat Messenger logs, created, saved, or altered on or after January 1, 2021, sent to, from, and/or through the email address (es) of, belonging to, or associated with the above listed Snapchat user account(s), or through other associated accounts.

e. Any and all 'Friend' activity, namely other Snapchat user accounts whose users have chosen to 'friend,' 'follow,' 'following' or otherwise socially associate their profiles with the above listed Snapchat user account(s) in order to communicate or otherwise interact with the individual user(s) created, saved, or altered on or after January 1, 2021,. This list includes 'friend,' 'follow,' 'following' currently associated with the account and past, or any such 'deleted' activity. Snapchat is to provide 'friends,' 'followers,' and 'following' of the above listed Snapchat user account, including complete user information, to include Friend ID account numbers, any vanity URLs, and/or profile names of the profile's current and 'deleted' friend listing.

f. Any and all messages, created, saved, or altered on or after January 1, 2021, sent to and from the above listed Snapchat user account(s), to include text and multi-media messages in the spam, archived, and 'other' mail folders.

g. Any and all Snapchat 'Groups' which the above listed Snapchat user account(s) is a member or otherwise associated.

h. Any and all search history created, saved, or altered on or after January 1, 2021, conducted by the above listed Snapchat user account(s) within the Snapchat user community.